9241

UNIVERSITE PARIS VI

THESE de DOCTORAT D'ETAT

SPECIALITE : MATHEMATIQUES

PRESENTEE PAR: Monsieur Mikhail DEZA

SUJET de la THESE

Quelques travaux sur la combinatoire et la théorie du codage algébrique.

soutenue le, 4-12-1973 devant la commission d'examen

JURY : MM. R.FORTET — Président
M. KRASNER — Examinateurs
C. BERGE
P. CAMION

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41549212_0019

UNIVERSITE PARIS VII

THESE de DOCTORAT D'ETAT

SPECIALITE : MATHEMATIQUES

PRESENTEE PAR: Monsieur Mikhail DEZA

SUJET de la THESE

Quelques travaux sur la combinatoire et la théorie du codage algébrique.

soutenue le, **devant la commission d'examen**

JURY: MM. R.FORTET — Président
M. KRASNER — Examinateurs
C. BERGE
P. CAMION

UNIV.
LEIDEN
BIB.

COMBINATOIRE. — *Matrices des formes quadratiques non négatives pour des arguments binaires.* Note (*) de M. **Mikhaïl Deza**, présentée par M. André Lichnerowicz.

On montre que ces matrices forment un cône convexe avec un nombre fini de générateurs; par la proposition 4 ci-dessous, ce cône doit caractériser les matrices entières $m \times m$ dont les coefficients sont les distances de Hamming deux à deux de m mots binaires. On construit une famille particulière de générateurs de ce cône.

Soit H_m l'ensemble de toutes les matrices réelles symétriques $((h_{ij}))_m^m$ telles que $\sum_{i,j} h_{ij} x_i x_j \geqq 0$ pour tous $x_1, \ldots, x_m = 0$ ou 1.

La description de l'ensemble H_m a un intérêt pratique du fait des propositions suivantes (1)-(4) qui relient aux schémas combinatoires et aux codes binaires. Pour toute matrice binaire $Y = ((y_{pq}))$ de m lignes et de n colonnes, nous posons

$$s_{ij}(Y) = \sum_{1 \leqq t \leqq n} y_{it} y_{jt} \qquad \text{(produit scalaire des lignes } i \text{ et } j\text{)},$$

$$r_{ij}(Y) = \sum_{1 \leqq t \leqq n} |y_{it} - y_{jt}| \qquad \text{(distance de Hamming des lignes } i \text{ et } j\text{)},$$

$$r_{0j}(Y) = \sum_{1 \leqq t \leqq n} y_{jt}.$$

On a :

(1) Si $((h_{ij}))_m^m$ est une matrice réelle symétrique, alors $((h_{ij})) \in H_m$ est équivalent à $\sum_{1 \leqq i \leqq j \leqq m} h_{ij} s_{ij}(Y) \geqq 0$ pour toute matrice binaire Y.

(2) Si $((h_{ij}))_m^m$ est une matrice réelle symétrique, alors $((h_{ij})) \in H_m$ est équivalent à $-\sum_{1 \leqq i \leqq j \leqq m} h_{ij} r_{ij}(Y) + \sum_{1 \leqq j \leqq m} \left(\sum_{1 \leqq f \leqq m} h_{fj} \right) r_{0j}(Y) \geqq 0$ pour toute matrice binaire Y.

(3) Si $((\tilde{s}_{ij}))$, $1 \leqq i, j \leqq m$ est une matrice rationnelle symétrique, alors on a $\forall\, i, j,\ i \neq j$, $\tilde{s}_{ij} = k^{-1} s_{ij}(Y)$ [c'est-à-dire $((\tilde{s}_{ij})) = k^{-1} YY^T$] pour un entier $k > 0$ et une matrice binaire Y, si et seulement si $\sum_{1 \leqq i \leqq j \leqq m} h_{ij} \tilde{s}_{ij} > 0$ pour toute $((h_{ij})) \in H_m$.

(4) Si $((\tilde{r}_{ij}))$, $0 \leqq i, j \leqq m$, est une matrice rationnelle symétrique, alors on a $\forall\, i, j,\ i \neq j$, $\tilde{r}_{ij} = k^{-1} r_{ij}(Y)$ pour un entier $k > 0$ et une matrice binaire Y si et seulement si

$$-\sum_{1 \leqq i \leqq j \leqq m} h_{ij} \tilde{r}_{ij} + \sum_{1 \leqq j \leqq m} \left(\sum_{1 \leqq i \leqq m} h_{fj} \right) \tilde{r}_{0j} \geqq 0 \quad \text{pour toute } ((h_{ij})) \in H_m.$$

Remarquons, en ce qui concerne la proposition 3, que si $\tilde{s}_{ij} = k^{-1} s_{ij}(Y)$, $\forall\, i, j$, il existe *a fortiori* une matrice *réelle* Z telle que tous $\tilde{s}_{ij} = s_{ij}(Z)$, et en vertu de (1) cela est équivalent à $\sum_{i,j} \tilde{s}_{ij} x_i x_j \geqq 0$ pour tous réels $x_1, \ldots, x_m$. L'affirmation inverse n'est pourtant pas vraie; par exemple, $Z' Z'^T = ((s'_{ij}))$, où Z' est une matrice réelle, mais $\sum_{i \leqq j} h'_{ij} s'_{ij} = -1 < 0$ où $((h'_{ij})) \in H_m$, pour

$$((s'_{ij})) = \begin{bmatrix} 4 & 2 & 2 & 2 \\ 2 & 4 & 2 & 2 \\ 2 & 2 & 2 & 1 \\ 2 & 2 & 1 & 2 \end{bmatrix}, \qquad ((h'_{ij})) = \begin{bmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix},$$

$$Z' = \begin{bmatrix} \sqrt{2} & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & \sqrt{2} & 0 \\ 0 & 1 & 1 & 0 & 0 \\ \sqrt{1/2} & 1/2 & 1/2 & \sqrt{1/2} & \sqrt{1/2} \end{bmatrix}.$$

Pour chacun des nombres $t = 1, \ldots, 2^m-1$, soient

$$t = \sum_{1 \leqq s \leqq m} g_{tf} 2^{f-1}, \qquad G(t) = ((g_{ti} g_{tj}))_m^m$$

et $\overline{G}_m$ l'ensemble de toutes les 2^m-1 matrices $G(t)$. Soit $\overline{H}_m$ l'ensemble de toutes les matrices $((h_{ij}))$ de H_m telles que :

(*a*) il existe exactement $\binom{m+1}{2}-1$ matrices linéairement indépendantes $G(t_q)$ de G_m telles que $\sum_{i,j} h_{ij} g_{t_q i} g_{t_q j} = 0$ pour tous $1 \leqq q \leqq \binom{m+1}{2}-1$;

(*b*) tous les nombres h_{ij} sont des entiers et 1 est leur unique diviseur commun.

THÉORÈME 1. — *L'ensemble* H_m *est un cône convexe pointé de dimension* $\binom{m+1}{2}$ *sur le champ de réels;* $\overline{H}_m$ *est un ensemble minimum de générateurs pour* H_m.

Effectivement, $((h_{ij})) \in H_m \Leftrightarrow \sum_{i,j} h_{ij} g_{ti} g_{tj} \geqq 0$ pour tous $G(t) \in \overline{G}_m$. Donc, H_m est un cône convexe, dual (sur le champ de réels) à un cône convexe pointé G_m avec un ensemble de générateurs $\overline{G}_m$ (on peut montrer que $\overline{G}_m$ est l'ensemble minimum de générateurs pour G_m). La dimension du cône G_m est $\binom{m+1}{2}$, puisque l'ensemble des $\binom{m+1}{2}$ matrices de $G(t)$ obtenues en donnant à t, les valeurs $t = 2^q$ ou $t = 2^q+2^p$ est libre. D'après le théorème 7 de ([2]), $\overline{H}_m$ est l'ensemble minimum de générateurs pour H_m. Les propositions 1, 2, 3 et 4, découlent du théorème 1.

Si $b = (b_1, \ldots, b_m)$, où tous b_i sont des entiers, alors soit $Q(b) = ((q_{ij}(b)))_m^m$, où $q_{ij}(b) = b_i b_j$ pour $i \neq j$ et $q_{ii}(b) = (b_i-1) b_i$.

Toutes les matrices de $\overline{H}_m$ connues pour le moment de l'auteur ont la forme $Q(b)$. On se propose par le théorème 3 de déterminer des générateurs de H_m parmi les matrices de $Q(b)$.

THÉORÈME 2. — *On a* $Q(b) \in H_m$ *pour tout* $b = (b_1, \ldots, b_m)$ *où tous* b_i *sont des entiers.*

Effectivement, pour tout $t \in [1, 2^m-1]$ on a

$$\sum_{i,j} q_{ij}(b) g_{ti} g_{tj} = \sum_{1 \leqq i \leqq m} b_i(b_i-1) g_{ti} g_{ti} + \sum_{1 \leqq i \neq j \leqq m} b_i b_j g_{ti} g_{tj} = \left(\sum_{1 \leqq i \leqq m} b_i g_{ti} \right) \left(\sum_{1 \leqq i \leqq m} b_i g_{ti} - 1 \right) \geqq 0.$$

THÉORÈME 3. — *Soit* $b = ((b_1, \ldots, b_m)$, *où* $b_1 \geqq \ldots \geqq b_m$, *tous les* b_i *sont des entiers* $\neq 0$; *soit* f *le nombre de* b_i *positifs.*

(1) *Si* $f \notin [2, m-2]$, *alors* $Q(b) \in \overline{H}_m$ *seulement pour :*

(*a*) $b = (1, 1)$ *ou* $(1, -1)$ *ou* $(1, 1-1)$;

(*b*) $f = m-1$, $b_1 = 1$, $b_m \geqq -m+3$.

DISCRETE MATHEMATICS 6 (1973) 000–000. © North-Holland Publishing Company

UNE PROPRIETE EXTREMALE DES PLANS PROJECTIFS FINIS DANS UNE CLASSE DE CODES EQUIDISTANTS

M. DEZA

C.N.R.S. Paris, France

Reçu le 1 novembre 1972 *

Résumé. Soit $X \subset F_2^n$ où F_2 est le champ de Galois à deux éléments. Si $r(x, y)$ est la distance de Hamming entre $x, y \in F_2^n$, $|S|$ est le nombre d'éléments de l'ensemble S et $E \cup F = X$, alors

$$\sum_{x \in E,\, y \in F} r(x, y) \geq \frac{|F|}{2|E|} \sum_{x,\, y \in E} r(x, y) + \frac{|E|}{2|F|} \sum_{x,\, y \in F} r(x, y) .$$

A l'aide de cette inégalité, on démontre l'inexistence de codes équidistants non triviaux de m mots et de distance $2k$ où $m \geq k^2 + k + 3$. Le code non trivial de $k^2 + k + 2$ mots existe, si une PG$(2, k)$ existe; J.H. van Lint, dans [4], a démontré l'implication inverse. En termes de problème extrémal, on montre que le nombre maximal de mots d'un code équidistant de longueur n et de distance $2k$ est égal à $[n/k]$ pour $n \geq k(k^2 + k + 2)$.

1. Introduction

On dit qu'une matrice binaire à m lignes et n colonnes dans laquelle deux lignes différentes ne coïncident pas exactement en d positions correspondantes (c'est-à-dire que la distance de Hamming entre les lignes est égale à d) est un *code équidistant* de m *mots*, de *distance* d et de *longueur* n ou, en abrégé, un (m, d, n)-*code*. Dans la suite, pour distance d, on prendra un nombre pair , puisqu'on peut facilement vérifier que pour $m > 2$ et d impair, un (m, d, n)-code n'existe pas. Nous appellerons $(m, 2k)$-code tout code équidistant de m mots et de distance $2k$. Pour $m > 2$, un $(m, 2k)$-code est appelé *trivial*, si pour tout $i \in [1, m]$ il contient exactement k colonnes $(x_{1s}, ..., x_{ms})^T$ telles que $x_{1s} = ... = x_{i-1\,s} = 1 - x_{i+1\,s} = ... = x_{ms}$ et par ailleurs peut-être, des colonnes de 0 et de 1. Il est évident qu'un $(m, 2k)$-code trivial existe pour tous

* Première version reçue le 2 juin 1972.

(2) *Si* $f \in [2, m-2]$, $b_m = -1$, *alors* $Q(b) \in \overline{H}_m$ *seulement pour :*

(*c*) $f = 2$, $m-f \geqq b_1+b_2$;

(*d*) $b_1 = b_f$, $n-f \geqq b_1+b_2$;

(*e*) $b_1 > b_f$, $f > 2$, $m-f \geqq b_1+b_2-1$.

(3) *Si* $f \in [2, m-2]$, $b_m \neq -1 = -b_1$, *alors* $Q(b) \in \overline{H}_m$ *seulement pour :*

(*g*) $f \geqq -b_{m-1}-b_m$.

A ce propos, le cas (*a*) dans les termes de la proposition 2 correspond à la règle du triangle pour la métrique de Hamming.

Envisageons les applications suivantes de b :

(1) $b^{(1)}$ obtenu de b en ajoutant ou retranchant des zéros;

(2) $b^{(2)}$ obtenu de b par une permutation des éléments :

(3) $b^{(3)}$ obtenu de b en remplaçant l'un des éléments par $1-\sum_{1 \leqq f \leqq m} b_f$;

(4) $b^{(4)}$ obtenu de b en remplaçant tous les b_t par

$$\left(1-2\left|g_{ut}-\sum_{1 \leqq q \leqq m} g_{uq}\, b_q\right|\right) b_t \qquad \text{où} \quad u \in [1, 2^m-1]$$

et

$$\sum_{1 \leqq q \leqq m} g_{uq}\, b_q = 0 \quad \text{ou} \quad 1.$$

THÉORÈME 4. — *Si* $Q(b) \in \overline{H}_m$, *alors* $Q(b^{(1)})$, $Q(b^{(2)})$, $Q(b^{(3)})$, $Q(b^{(4)}) \in \overline{H}_m$.

Voici les b connus pour $m \leqq 7$, tels que $Q(b) \in \overline{H}_m$; pour exclure également l'application de $b^{(3)}$ ils sont notés sous la forme $(b_0, b_1, \ldots, b_m)$ où

$$b_0 = 1-\sum_{1 \leqq f \leqq m} b_f.$$

$(1, 1, -1)$; $(1, 1, 1, -1, -1)$; $(1, 2, 1, -1, -1, -1)$; $(1, 3, 1, -1, -1, -1, -1)$;
$(1, 2, 2, -1, -1, -1, -1)$; $(1, 2, 1, 1, -1, -1, -2)$; $(1, 1, 1, 1, -1, -1, -1)$;
$(1, 4, 1, -1, -1, -1, -1, -1)$; $(1, 3, 2, -1, -1, -1, -1, -1)$;
$(1, 3, 1, 1, -1, -1, -1, -2)$; $(1, 3, 1, 1, 1, -2, -2, -2)$;
$(1, 2, 2, 1, -1, -1, -1, -2)$; $(1, 2, 1, 1, -1, -1, -1, -1)$;
$(3, 2, 2, -1, -1, -1, -1, -2)$; $(2, 2, 2, -1, -1, -1, -1, -1)$.

Pour $m \leqq 4$ ces b (avec leur $b^{(1)}$, $b^{(2)}$, $b^{(3)}$, $b^{(4)}$) épuisent $\overline{H}_m$.

Soit $((s_{ij}))_m$ une matrice symétrique d'entiers. Par (1), une condition nécessaire pour l'existence d'une matrice binaire Y, telle que $((\bar{s}_{ij})) = YY^T$, est que $\forall ((h_{ij})) \in \overline{H}_m$, $\sum_{i,j} \bar{s}_{ij}\, h_{ij} \geqq 0$. Lorsque $m \leqq 4$, cette condition devient suffisante.

Les preuves des théorèmes 3 et 4 figurent dans un document de 15 pages qui sera conservé 5 ans par les Archives de l'Académie et dont copie peut être obtenue de l'Académie.

(*) Séance du 27 août 1973.

(1) G. YOUNG et A. S. HOUSEHOLDER, *Discussion of a set of points in terms of their mutual distances* (*Psychometrica*, 3, 1938, p. 331-333).

(2) A. J. GOLDMAN et A. W. TUCKER, *Polyhedral convex cones*, dans *Linear inequalities and related systems*, Princeton University Press, 1936.

31, *rue Borghèse*,
92200 *Neuilly-sur-Seine*.

$m > k \geq 1$. Le but de ce travail est de trouver un critère d'existence des $(m, 2k)$-codes non-triviaux et son utilisation. Ces résultats sont la suite du travail [2]. Les affirmations du Théorème 2.1 et le point (iii) du Théorème 1.1 ont été données sans démonstration dans [3, pp. 84–85].

Les codes équidistants sont utilisés dans de nombreux problèmes liés au codage, à la recherche, à la fiabilité d'automates finis etc. Ils représentent une généralisation étendue de blocs-schémas incomplets équilibrés. Précisément, si A est une matrice d'incidence de configuration $-(b, v, r, \overline{k}, \lambda)$ il est évident que A^T est un $(m, 2k, n)$-code avec $m = v$, $2k = 2(r - \lambda)$ et $n = b$, dans lequel le poids de chaque ligne est r et le poids de chaque colonne est $\overline{k}$. Si $r \geq 2\lambda$, alors en ajoutant à la matrice A^T $(r - 2\lambda)$ colonnes de 1, et ensuite une ligne de 0, nous obtenons un $(m, 2k, n)$-code avec $m = v + 1$, $2k = 2(r - \lambda)$ et $n = b + r - 2\lambda$, dans lequel $(r - 2\lambda)$ colonnes ont le poids $(m - 1)$, le poids des autres colonnes étant égal à $\overline{k}$. Dans [4], on montre que l'existence d'une PG(2, k) équivaut à l'existence d'un $(k^2 + k + 2, 2k)$-code non trivial. Il est aisé de démontrer que l'existence d'une matrice d'Hadamard d'ordre $4k$ équivaut à l'existence d'un $(4k, 2k, 4k - 1)$-code.

En termes de $(m, 2k)$-codes, les résultats de cet ouvrage sont résumés dans le théorème suivant (qui sera démontré dans le Paragraphe 3).

Théorème 1.1. *Soient m et k deux entiers tels que $m > k \geq 1$, alors on a:*

(i) *Il existe un nombre $N(m, k)$ tel que la condition nécessaire et suffisante pour l'existence d'un $(m, 2k, n)$-code est $n \geq N(m, k)$.*

(ii) *$N(m, k) \leq m\,k$ et il existe un nombre $f(k)$ tel que $f(k) \geq 4$ et $N(m, k) = m\,k$ si et seulement si $m \notin [4, f(k)]$.*

(ii)' *Il existe un $(m, 2k)$-code trivial et sa longueur est supérieure ou égale à $m\,k$. Il existe un $(m, 2k)$-code, différent d'un code trivial si et seulement si $m \in [4, f(k)]$.*

(iii) *$f(k) \leq k^2 + k + 2$ et $f(k) = k^2 + k + 2$ s'il existe une* PG(2, k).

Le problème du calcul exact du nombre $f(k)$ reste ouvert. Le seule pas en avant dans cette direction est l'estimation $f(k) < k^2 + k + 2$ pour le cas de l'inexistence d'une PG(2, k), aimablement communiqué à l'auteur par J.H. van Lint. De cette façon, dans le problème du calcul du nombre maximal de mots du code équidistant de distance $2k$ (de même que dans le problème du calcul du nombre maximal de carrés latins orthogonaux), l'obtention d'un maximum équivaut à l'existence d'une PG(2, k). Dans le Paragraphe 4 on envisage le cas $f(k) = f(k - 1)$.

On appelle le nombre $N(m, k)$, introduit au point (i) du Théorème 1.1, une *longueur minimum* d'un $(m, 2k)$-code. On voit, à l'aide des points (ii) et (iii) du Théorème 1.1, que $N(m, k) = m\,k$ pour $m \notin [4, k^2 + k + 2]$; on peut aussi démontrer que $N(4, k) = 3k$ et $N(m, 2) = 7$ pour $m \in [5, 8]$ (le $(8, 4, 7)$-code est formé de la ligne de 0 et de toutes les permutations cycliques de la ligne 0 0 1 0 1 1 1). Ainsi le problème du calcul du nombre $N(m, k)$ reste ouvert uniquement pour $m \in [5, k^2 + k + 2]$, $k \geq 3$.

Il existe aussi un nombre $M(k, n)$ tel qu'un $(m, 2k, n)$-code (pour $n \geq 2k \geq 2$) existe, si et seulement si l'inégalité $m \leq M(k, n)$ a lieu. L'inégalité $M(k, n) \geq [n/k]$ découle aisément du point (ii) du Théorème 1.1; de plus, $M(k, n) = [n/k]$ pour $n \notin (3k - 1, k f(k) - 1]$ et $M(k, n) > [n/k]$ pour $n \in (3k - 1, k f(k) - 1]$ dans le cas $n \equiv k - 1 \pmod{k}$. De l'inégalité $f(k) \leq k^2 + k + 2$ du Théorème 1.1 découle l'égalité donnée dans le résumé: $M(k, n) = [n/k]$ pour $n \geq k(k^2 + k + 2)$. Il existe aussi le nombre $K(m, n)$ qui est la distance maximum d'un code équidistant de m mots et de longueur n. Or la condition $k \leq K(m, n)$ n'est pas suffisante pour l'existence de $(m, 2k, n)$-codes.

2. Certaines propriétés des matrices binaires

Nous présentons ici les Théorèmes 2.1 et 2.2 que nous allons utiliser dans le Lemme 3.1. (Le Théorème 2.1 montre que les distances de Hamming entre les lignes de toute matrice binaire sont d'une certaine façon "balancées" par certaines inégalités linéaires par rapport aux distances. La recherche de ces inégalités et de leurs pareilles est un problème autonome intéressant.) Soient:

$X = \|x_{ij}\|_m^n$ une matrice binaire à m lignes et n colonnes ($m \geq 2$);
$r_{pq} = \sum_{j=1}^{n} |x_{pj} - x_{qj}|$ pour tous entiers $p, q \in [1, m]$ (c'est la distance de Hamming);
$a = \min r_{pq}$ (où $1 \leq p < q \leq m$), $b = \max r_{pq}$ (où $1 \leq p < q \leq m$);
$(i_1, \ldots, i_m)$ une permutation des nombres $1, \ldots, m$;
f un entier de $[1, m - 1]$, s un entier de $[1, n]$;
$t_s = \min(\sum_{i=1}^{m} x_{is}, m - \sum_{i=1}^{m} x_{is})$ le poids généralisé de la s-ième colonne;
τ_s le nombre de colonnes de X coïncidant avec sa s-ième colonne.

Théorème 2.1. *Pour une matrice X, une permutation $(i_1, ..., i_m)$ et un nombre f, on a*

$$\sum_{1 \le p \le f < q \le m} r_{i_p i_q} - \frac{m-f}{f} \sum_{1 \le p < q \le f} r_{i_p i_q} - \frac{f}{m-f} \sum_{f+1 \le p < q \le m} r_{i_p i_q} \ge 0 .$$

En effet, de la définition du nombre r_{pq}, il est clair qu'il est suffisant de démontrer l'inégalité pour le cas $n = 1$ (c'est-à-dire que X est une colonne binaire). Cette colonne contient e_1 unités dans les endroits $i_1, ..., i_f$ et e_2 unités dans les endroits $i_{f+1}, ..., i_m$; soient $g_1 = e_1/f$, $g_2 = e_2/(m-f)$. Alors l'inégalité prendra la forme

$$\begin{aligned} & e_1(m-f-e_2) + e_2(f-e_1) - e_1(f-e_1)(m-f)/f - \\ & \quad e_2(m-f-e_2)f/(m-f) = \\ & \quad g_1(1-g_2) + g_2(1-g_1) + g_1(1-g_1) + g_2(1-g_2) = \\ & \quad (g_1-g_2)^2 \ge 0 . \end{aligned}$$

Théorème 2.2. *Pour une matrice X et un nombre s tel que $t_s \neq 0$, on a*

$$\tau_s \le b - a + a\,m/2t_s(m-t_s) .$$

En effet, désignons par $\bar{X}$ une matrice binaire, obtenue de la matrice X, par élimination de toutes les τ_s colonnes, coïncidant avec sa s-ième colonne. Considérons une permutation $(\bar{i}_1, ..., \bar{i}_m)$ et un nombre $\bar{f}$ tels que $x_{i_p s} = 1$ pour $p \in [1, \bar{f}]$ et $x_{i_p s} = 0$ pour $p \in [\bar{f}+1, m]$. Il est évident que $\bar{f} \in [1, m-1]$, puisque $t_s = \min(\bar{f}, m-\bar{f})$ d'après le choix de la permutation, et que $t_s \neq 0$ par définition. Désignons la distance de Hamming entre les q-ième et p-ième lignes $(1 \le p < q \le m)$ de la matrice $\bar{X}$ par $\bar{r}_{pq}$. Il est évident que

$$\bar{r}_{\bar{i}_p \bar{i}_q} = r_{\bar{i}_p \bar{i}_q} - \tau_s \le b - \tau_s \quad \text{si } 1 \le p \le \bar{f} < q \le m$$

et que

$$r_{\bar{i}_p \bar{i}_q} = r_{\bar{i}_p \bar{i}_q} \geq a \qquad \text{si } 1 \leq p < q \leq \bar{f}$$

$$\text{ou } \bar{f} + 1 \leq p < q \leq m .$$

En appliquant le Théorème 2.1 à la matrice binaire $\bar{X}$, à la permutation $(\bar{i}_1, \ldots, \bar{i}_m)$ des numéros de ses lignes et au nombre $\bar{f}$, nous obtenons

$$0 \leq \bar{f}(m-\bar{f})(b-\tau_s) - \frac{m-\bar{f}}{\bar{f}} \binom{\bar{f}}{2} a - \frac{\bar{f}}{m-\bar{f}} \binom{m-\bar{f}}{2} a =$$

$$\bar{f}(m-\bar{f})(b-\tau_s-a) + \tfrac{1}{2}ma$$

d'où on a l'inégalité cherchée puisque $t_s = \min(\bar{f}, m-\bar{f})$ par le choix de la permutation et du nombre $\bar{f}$; d'où $\bar{f}(m-\bar{f}) = t_s(m-t_s)$.

Il est aisé de vérifier que pour $t_s \neq 0$ on a:

$$m \leq \frac{t_s^2}{t_s - \frac{1}{2}a(\tau_s - b + a)}$$

si $\tau_s > (b-a) + a/2t_s$.

3. Démonstration du théorème principal

Lemme 3.1. *Pour tout $(m, 2k, n)$-code et tout entier s, $1 \leq s \leq n$, on a $t_s(m-t_s) \leq m\,k$.*

En effet, en appliquant le Théorème 2.2 au $(m, 2k, n)$-code, nous obtenons $\tau_s\, t_s(m-t_s) \leq m\,k$ puisque $b = a = 2k$. Mais $\tau_s \geq 1$ et le lemme est évident.

Lemme 3.2. *Pour tout $(m, 2k, n)$-code X tel que $t_s \leq [(m+2k-1)/(k+1)] - 1$ (pour tout $1 \leq s \leq n$) on a $t_s \leq 1$ pour tout $1 \leq s \leq n$.*

En effet, sans perte de généralité, on peut supposer que X comprend une ligne de 0. Au cours de la démonstration, on utilise les propriétés évidentes d'un code équidistant de m mots et de distance $2k$, possédant

une ligne de 0:

(i) chaque ligne différente de la ligne de 0 contient $2k$ unités;

(ii) deux lignes quelconques différentes de la ligne de 0 ont k unités communes (dans les positions correspondantes).

Soit $[(m + 2k - 1)/(k + 1)] = t$. Il est évident que:

(a) $t_s < t$ $(1 \leq s \leq n)$;

(b) $m \geq k(t - 2) + t + 1$.

En raison de la condition (a), la matrice X ne contient que des colonnes ayant au plus $t - 1$ unités (appelons-les colonnes de type I) et des colonnes ayant au moins $m - t + 1$ unités (appelons-les colonnes de type II). Ces deux ensembles de colonnes sont disjoints. Pour démontrer le lemme, il suffit de montrer que X satisfait aux conditions suivantes:

(i)′ le nombre de colonnes du type II est inférieur ou égal à k;

(ii)′ toute ligne différente de la ligne de 0 ne contient pas moins de k unités dans les colonnes de type II.

En effet, au cas où sont réalisées les conditions (i)′ et (ii)′, la matrice X contient exactement k colonnes de type II dont chacune a $(m - 1)$ unités et exactement $(m - 1)k$ colonnes du type I dont chacune a 1 unité, d'où $t_s \leq 1$, $1 \leq s \leq n$. Supposons que X contient au moins $k + 1$ colonnes de type II. Toute colonne de type II contient au plus $t - 2$ zéros dans les lignes différentes de la ligne de 0. D'après (b), on a $(m - 1) - (k + 1)(t - 2) \geq 2$, c'est-à-dire qu'il existe 2 lignes (différentes de la ligne de 0) qui contiennent des unités dans les mêmes $(k + 1)$ colonnes de type II, ce qui contredit la propriété (ii) de la matrice X. Montrons que la condition (ii)′ est remplie. Soit u une ligne différente de la ligne de 0 de la matrice X et supposons que u contient exactement q unités dans les colonnes de type II. Il suffit de démontrer que $q \geq k$. En raison de la propriété (i) de la matrice X $(2k - q)$ colonnes de type I contiennent une unité dans la ligne u. Soit X' une matrice constituée de toutes les lignes différentes de u, et de la ligne de 0 de la matrice X et de toutes les colonnes de la matrice X contenant une unité dans la ligne u. D'après la définition des colonnes de type I et de type II, la matrice X' contient au plus $q(m - 2)$ unités par colonnes de type II et au plus $(2k - q)(t - 2)$ unités par colonnes de type I. En vertu de la propriété (ii) de la matrice X, la matrice X' contient $k(m - 2)$ unités. Donc, $(2k - q)(t - 2) + q(m - 2) \geq k(m - 2)$ d'où $q \geq k - k(t - 2)/(m - t)$. Mais $k(t - 2) < m - t$ d'après (b) et q est un entier, d'où $q \geq k$.

Lemme 3.3. *Tout $(m, 2k, n)$-code, tel que $m \notin [4, k^2 + k + 2]$ remplit la condition $t_s \leq 1$ pour $s \in [1, n]$.*

En effet, pour $m \geq k^2 + k + 3$ et $t_s \geq k + 2$, on a (en tenant compte que $k \geq 1$) $t_s(m - t_s) - mk \geq (k + 2)(k^2 + 1) - (k^2 + k + 3)k > 0$. Cela contredit le Lemme 3.1 et donc, $t_s < k + 2$. De $t_s \leq k + 1$ et du fait que $[(m + 2k - 1)/(k + 1)] - 1 \geq k + 1$ pour $m \geq k^2 + k + 3$, il résulte que la condition du Lemme 3.2 est remplie dans ce cas et par conséquent $t_s \leq 1$ pour $1 \leq s \leq n$. L'inégalité $t_s \leq 1$ pour $m = 2, 3$ résulte du fait que $t_s \leq m - t_s$.

Lemme 3.4. *Un $(m, 2k, n)$-code est trivial si et seulement si $t_s \leq 1$ pour $1 \leq s \leq n$.*

En effet, la nécessité découle de la définition du nombre t_s et du $(m, 2k)$-code trivial. Soit maintenant un $(m, 2k, n)$-code qui remplit la condition $t_s \leq 1$ $(1 \leq s \leq n)$. Cela signifie qu'il contient tout au plus h_i, $1 \leq i \leq m$, colonnes $(x_{1s}, \ldots, x_{ms})^T$ telles que $x_{1s} = \ldots = x_{i-1s} = 1 - x_{is} = x_{i+1s} = \ldots = x_{ms}$, c'est-à-dire $t_s = 1$ (à l'exception des colonnes de 0 et des colonnes de 1, c'est-à-dire des colonnes avec $t_s = 0$). Il reste à montrer que $h_1 = \ldots = h_m = k$. Il est évident que, pour tous i, j, tels que $i \neq j$ et $i, j \in [1, m]$ la distance r_{ij} entre la i-ième et la j-ième ligne de notre code est $2k = h_i + h_j$. Il résulte de la condition $m > 2$ qu'il existe un entier q dans $[1, m]$, différent de i et de j. On a $r_{iq} - r_{jq} = 2k - 2k = 0 = (h_i + h_q) - (h_j + h_q) = h_i - h_j$ d'où $h_1 = \ldots = h_m = k$.

Lemme 3.5. *Si $m \geq 4$ et s'il existe un $(m, 2k)$-code non trivial, alors, pour tout $m' \in [4, m]$, il existe un $(m', 2k)$-code non trivial.*

En effet, en vertu du Lemme 3.4, il y a dans un $(m, 2k)$-code non trivial une colonne s telle que $t_s \geq 2$ ou, en d'autres termes, la colonne s contient au moins 2 zéros et au moins 2 unités. Rejetons $(m - m')$ lignes du code des $(m - 4)$ qui restent en ne prenant pas en considération deux des lignes dans lesquelles la colonne s contient un zéro, et deux lignes dans lesquelles la colonne s contient une unité. C'est possible, puisque $m - m' \geq 0$ et $(m - 4) - (m - m') = m' - 4 \geq 0$. On obtient un $(m', 2k)$-code.

Lemme 3.6. *S'il existe un $(m, 2k)$-code non trivial, on a $N(m, k) < m\,k$. Dans le cas contraire, on $N(m, k) = m\,k$.*

En effet, le lemme est vrai dans le cas où tous les $(m, 2k)$-codes sont triviaux, du fait que tout $(m, 2k)$-code trivial contient au moins $m\,k$ colonnes, tandis qu'un $(m, 2k)$-code trivial, dans lequel il n'y a pas de colonnes s avec $t_s = 0$, contient exactement $m\,k$ colonnes. D'autre part, appliquant à un $(m, 2k)$-code l'estimation supérieure du [1, Théorème 5], on obtient $\bar{n} \leq \binom{m}{2} 2k/(m-1) = m\,k$, où $\bar{n}$ est le nombre de colonnes du $(m, 2k)$-code, telles que $t_s \neq 0$. De plus, d'après la démonstration de l'estimation supérieure du [1, Théorème 5], on voit que $n = m\,k$ si et seulement si le $(m, 2k)$-code ne possède que des colonnes qui n'ont pas plus d'une unité et des colonnes qui n'ont pas plus d'un zero, c'est-à-dire (en vertu du Lemme 3.4) au cas où le $(m, 2k)$-code est trivial. Donc, $N(m, k) \leq \bar{n} < m\,k$ si le $(m, 2k)$-code est non trivial.

A ce propos, il serait intéressant de décrire les spectres des nombres $\bar{n}$ (de longueurs propres) pour des $(m, 2k)$-codes non triviaux; pour un (5, 4)-code ce spectre est lacunaire (mais pas pour $m \leq 4$).

Passons maintenant à la *démonstration du Théorème* 1.1. De l'existence du $(m, 2k, n)$-code découle l'existence du $(m, 2k, n')$-code pour tous entier $n' \geq n$ (on peut obtenir ce code en ajoutant au code $n' - n$ colonnes de 0). D'autre part, un $(m, 2k, n)$-code n'existe plus pour $n < 2k$. Désignons par $N(m, k)$ le plus petit des entiers n, non inférieurs à $2k$, tels que un $(m, 2k, n)$-code existe. La propos. 1 du théorème est établie. De l'existence d'un $(m, 2k)$-code trivial de longueur $m\,k$, il résulte que $N(m, k) \leq m\,k$. D'après le Lemme 3.6, il vient que la condition nécessaire et suffisante pour l'inexistence d'un $(m, 2k)$-code non trivial est $N(m, k) = m\,k$. En vertu des Lemmes 3.3 et 3.4 pour $m \notin [4, k^2 + k + 2]$ il n'existe pas de $(m, 2k)$-code non trivial. Puis, en vertu du Lemme 3.5 et du fait évident de l'existence d'un $(4, 2k)$-code non trivial, on est amené à l'existence d'un maximum parmi les entiers i de $[4, k^2 + k + 2]$ (désignons ce maximum par $f(k)$) tels qu'il existe un $(i, 2k)$-code non trivial. S'il existe une PG$(2, k)$, alors en ajoutant à sa matrice d'incidence $(k-1)$ colonnes de 1, et ensuite une ligne de 0, nous obtenons un $(k^2 + k + 2, 2k)$-code. Par conséquent, $f(k) = k^2 + k + 2$ dans ce cas et le Théorème 1.1 est démontré.

4. $(m, 2k)$-codes infractionables

Nous appellerons un $(m, 2k)$-code *A fractionable* s'il existe un nombre q, $1 \leq q < k$, tel qu'un certain nombre de colonnes du code A forme un $(m, 2q)$-code. Tout $(m, 2k)$-code trivial est infractionable seulement pour $k = 1$; tout $(m, 2k)$-code est fractionable pour $k \geq 2$, $m = 2, 3, 4$. Si le nombre k, $k \geq 2$, est fixé et s'il existe des nombres m pour lesquels certains $(m, 2k)$-codes sont infractionables, nous désignerons par $\tilde{f}(k)$ le maximum de ces nombres; on a alors: $\tilde{f}(k) \leq f(k)$.

Lemma 4.1. *Pour $k \geq 2$, l'inégalité $f(k) \geq f(k-1)$ devient une égalité si et seulement s'il existe un $(f(k), 2k)$-code non trivial fractionable.*

Effectivement, si $f(k) = f(k-1)$, le $(f(k), 2k)$-code non trivial fractionable est obtenu en ajoutant un certain $f(k-1), 2)$-code à un certain $(f(k-1), 2(k-1))$-code non trivial. Démontrons maintenant la suffisance. Supposons qu'il existe un $(f(k), 2k)$-code non trivial fractionnable. En vertu de la définition de la fractionnabilité, on peut ôter de ce code quelques colonnes de façon à obtenir un $(f(k), 2q)$-code non trivial où $q \leq k-1$. Donc $f(k) \leq f(q)$ d'après la définition de la fonction $f(x)$; enfin, $f(k) = f(q)$ puisque la fonction $f(x)$ n'est pas décroissante.

D'après le lemme, on voit que $\tilde{f}(k) = f(k)$ si $f(k) > f(k-1)$. En particulier $\tilde{f}(k) = f(k) = k^2 + k + 2$ s'il existe une PG(2, k). Pour $k = 6$, après avoir examiné une (25, 9, 3)-configuration, nous obtenons $26 \leq \tilde{f}(6) \leq f(6) \leq 43$.

Il serait intéressant de décrire tout le spectre des nombres m, $m \in [5, f(k)]$, pour lesquels il existe un $(m, 2k)$-code infractionable. Soit R_m, $m \geq 2$, l'ensemble de tous les $(m, 2k)$-codes standards (c'est-à-dire avec une première ligne de zéros, sans colonnes de zéros et avec une même ordonnance de colonnes), où k est un nombre naturel. Nous appellerons "produit" de tous les éléments $a, b \in R_m$, le code ab, dont l'ensemble de colonnes est la réunion des ensembles des colonnes des codes a et b. Nous désignerons par a_2 le $(m, 2)$-code trivial. Alors l'ensemble R_m devient un demi-groupe commutatif, tout code trivial devient une puissance de l'élément a_2 et les codes nonfractionable sont analogues aux nombres premiers dans le demi-groupe multiplicatif des nombres naturels 2, 3, 4, ... On peut ordonner en partie le demi-groupe R_m à l'aide de la relation ordinaire d'ordre pour la demi-distance k.

Note

L'auteur est vivement reconnaissant à Mme Reine Fournier, de l'université de Montréal, pour ses bienveillantes corrections qui ont rendu son français plus intelligible.

Références

[1] M. Deza, Réalisabilité des matrices de distance dans des cubes unités, Problemy kibernet.7 (1962).
[2] M. Deza, Codes maximum équidistants de grande longueur, Résumés des exposés de la 2e conférence soviétique sur la théorie du codage, Bakou (1966).
[3] M. Deza, Propriétés linéaires métriques des codes binaires, Résumés des éxposés de la 4e conférence soviétique sur la théorie du codage, Tachkent (1969).
[4] J.H. van Lint, A theorem on equidistant codes, Discrete Math. 6 (1973) 000–000, present issue.

JOURNAL OF COMBINATORIAL THEORY (B) 16, 777–777 (1974)

DUPLICATE

Solution d'Un Problème de Erdös-Lovász

M. DEZA

31, rue P. Borghese, 92200 Neuilly-sur-Seine, France

Communicated by C. Berge

Received November 13, 1973

On démontre une conjecture de Erdös-Lovász selon laquelle pour toute famille d'ensembles $(A_1, ..., A_m)$ telle que les nombres $|A_i \cap A_j|$ sont égaux et que

$$m \geqslant \max_{1 \leqslant i \leqslant m} |A_i|^2 - \max_{1 \leqslant i \leqslant m} |A_i| + 2,$$

on a

$$A_i \cap A_j = \bigcap_{1 \leqslant g \leqslant m} A_g$$

pour tout $i < j$.

Le 8 janvier 1973, au séminaire du prof. C. Berge, à Paris, le prof. P. Erdös a posé le problème suivant:

Une famille d'ensembles $A = \{A_1, ..., A_m\}$ s'appelle:

un *Δ-système faible*, si les nombres $|A_i \cap A_j|$ sont les mêmes $(1 \leqslant i < j \leqslant m)$;

un *Δ-système fort*, si $A_i \cap A_j = \bigcap_{1 \leqslant g \leqslant m} A_g$ pour $1 \leqslant i < j \leqslant m$.

La conjecture de Erdös-Lovász énonce que *pour* $m \geqslant n^2 - n + 2$, *tout Δ-système faible est un Δ-système fort, où* $n = \max |A_i|$.

Montrons que la justesse de cette conjecture découle presque immédiatement du théorème 1 de [2]. Appelons $(m, 2k)$-*code* une (0, 1)-matrice de m lignes telle que deux lignes quelconques distinctes ne coïncident pas exactement dans $2k$ positions. Sans restreindre la généralité, on peut supposer que la première ligne n'est pas formée que de zéros. On appelle $(m, 2k)$-*code trivial* un $(m, 2k)$-code dans lequel toute colonne contient 0, 1, $m - 1$ ou m unités. Des propositions (2), (2'), (3) du théorème 1 de [2] (ces résultats ont été également exposés en 1969 et le résumé de l'exposé a été publié dans [1]) découle le résultat suivant:

THÉORÈME 1. *Pour tous les entiers* $m > k \geqslant 1$, *il existe un entier* $f(k)$

tel que, pour $m > f(k)$, *tout* $(m, 2k)$*-code est trivial. Plus précisément, on a* $4 \leqslant f(k) \leqslant k^2 + k + 2$.

Remarquons à ce propos que $f(k) = k^2 + k + 2$ si le plan projectif PG(2, k) existe; J. H. van Lint a démontré que $f(k) < k^2 + k + 2$ si PG(2, k) n'existe pas.

THÉORÈME 2. *Pour* $m \geqslant n^2 - n + 2$, *tout* Δ*-système faible* $A = \{A_1, \ldots, A_m\}$, *où* $n = \max |A_i|$, *est un* Δ*-système fort.*

En effet, posons $t = |A_i \cap A_j|$ $(1 \leqslant i < j \leqslant m)$ et $k = \max(t, n - t)$; $T(A)$ dénote une (0, 1)-matrice de $m + 1$ lignes et de

$$\left| \bigcup_{1 \leqslant i \leqslant m} A_i \right| + 2k - n$$

colonnes définie de la façon suivante: à la matrice d'incidence de famille A (aux ensembles A_i correspondent les lignes), adjoignons $k - t$ fois une matrice d'identité d'ordre m, puis $n - |A_i|$ colonnes (pour $1 \leqslant i \leqslant m$) avec 1 uniquement à la i-ième position, puis, adjoignons $k - (n - t)$ fois une colonne (1,..., 1) et enfin, adjoignons une ligne (0,..., 0). Il est clair que $T(A)$ est un $(m + 1, 2k)$-code. De plus, $T(A)$ est un $(m + 1, 2k)$-code trivial si et seulement si A est un Δ-système fort. Pour $t = 0, n$, A est toujours un Δ-système fort. Pour $0 < t < n$, on a $k \leqslant n - 1$, d'où $f(k) \leqslant f(n - 1)$. Comme $f(n - 1) \leqslant n^2 - n + 2 \leqslant m$ (l'inégalité de gauche découle du théorème 1, l'inégalité de droite est une condition donnée), nous obtenons $m + 1 > f(k)$, et par conséquent, (en vertu du théorème 1) $T(A)$ est un $(m + 1, 2k)$-code trivial; c'est-à-dire A est un Δ-système fort.

C.Q.F.D.

RÉFÉRENCES

1. M. DEZA, Lineĭnié métritcheskié svoĭstva dvoĭitchnykh kodov (en russe), Résumés des exposés de la 4^o conférence soviétique sur la théorie du codage, Moscou-Tachkent (1969).
2. M. DEZA, Une propriété extrémale des plans projectifs finis dans une classe de codes équidistants, *Discrete Math.* **6** (1973).